

## REMARKS

Claims 1, 5, 11-13, 16, 37, 41 and 42 are amended. Claims 17 and 18 are canceled. Claims 1-16 and 19-42 remain in the application. In view of the following remarks, Applicant respectfully requests withdrawal of the application and forwarding of the application on to issuance.

### Canceled Claims

Claims 17 and 18 have been canceled as having been duplicative.

### The Rejections

Claims 1, 5, 11-12, 37-42 stand rejected under 35 U.S.C §102(e) as being anticipated by U.S. Patent No. 6,678,733 to Brown et al. (hereinafter "Brown").

Claim 2 stands rejected under 35 U.S.C §103(a) as being obvious over Brown in view of U.S. Patent No. 6,070,243 to See et al. (hereinafter "See") and U.S. Patent No. 6,237,095 to Curry et al. (hereinafter "Curry").

Claims 3-4 and 6-10 stand rejected under 35 U.S.C §103(a) as being obvious over Brown in view of See.

Claims 13, 15 and 16-18 stand rejected under 35 U.S.C §103(a) as being obvious over Brown in view of U.S. Patent No. 6,584,564 to Olkin et al. (hereinafter "Olkin").

Claim 14 stands rejected under 35 U.S.C §103(a) as being obvious over Brown in view of Olkin and See.

Claims 19, 24 and 26 stand rejected under 35 U.S.C §103(a) as being obvious over Brown in view of U.S. Patent No. 6,345,347 to Biran.

1 Claims 20-22 stand rejected under 35 U.S.C §103(a) as being obvious over  
2 Brown in view of Biran and Olkin.

3 Claim 23 stands rejected under 35 U.S.C §103(a) as being obvious over  
4 Brown in view of Biran, Olkin and U.S. Patent No. 6,304,969 to Wasserman et al.  
5 (hereinafter "Wasserman").

6 Claim 25 stands rejected under 35 U.S.C §103(a) as being obvious over  
7 Brown in view of Biran and U.S. Patent No. 5,937,068 to Audebert.

8 Claims 27, 28, 30, 31, 33, 35 and 36 stand rejected under 35 U.S.C §103(a) as  
9 being obvious over Brown in view of Audebert and Olkin.

10 Claim 29 stands rejected under 35 U.S.C §103(a) as being obvious over  
11 Brown in view of Audebert, Olkin and Wasserman.

12 Claim 32 stands rejected under 35 U.S.C §103(a) as being obvious over  
13 Brown in view of Audebert, Olkin and Biran.

14 Claim 34 stands rejected under 35 U.S.C §103(a) as being obvious over  
15 Brown in view of Audebert, Olkin and See

16 Before undertaking a discussion of the substance of the Office's rejections,  
17 the following discussion of Brown is provided in an attempt to assist the Office in  
18 appreciating the patentable distinctions between the claimed subject matter and the  
19 references cited by the Office.

### 20 21 **The Brown Reference**

22 Brown discloses a walled garden that contains links to one or more servers  
23 providing network-based services. A walled garden proxy server (WGPS)  
24 controls access to the walled garden. When a user of a client wishes to access a  
25 service in the walled garden, the client sends a request to the WGPS including a

1 plot number identifying the service and a ticket granting the client access to the  
2 service. The WGPS denies access to clients lacking a ticket or presenting invalid  
3 tickets. In response, the client contacts a gateway server (GS) having a database  
4 of users and associated access rights. The user presents authentication information  
5 to the GS. If the user positively authenticates, the GS generates a ticket containing  
6 a Box ID from the client, an expiration date, and set of bits representing the access  
7 rights of the user. The GS encrypts the ticket and gives it to the client. When the  
8 WGPS receives a request to access a service in the walled garden, it decrypts the  
9 ticket and uses the plot number as an index into the set of bits representing the user  
10 access rights. The indexed value indicates whether the WGPS allows the client to  
11 access the service. Accordingly, services provided by the walled garden can be  
12 sold individually or in tiers.

13 Brown's ticket is illustrated in more detail in Fig. 8. There, the ticket 800 is  
14 shown to include a Box ID 810 of the client 112 requesting the ticket, a version  
15 number 812, an expiration date 814 (or duration when the ticket is valid), an  
16 affiliation 815, and a set of bits representing the access rights of the user 816. The  
17 version number 812 is a control number used by the GS 416 to ensure that the  
18 WGPS 414 properly interprets the ticket 800. The expiration date 814 can be any  
19 time in the future or a time span when the ticket 800 is valid and may range, for  
20 example, from a few minutes to a few hours. The affiliation indicates the  
21 particular walled garden 420 or MSO to which the ticket 800 pertains.

22 Brown instructs that the set of bits representing the access rights of the user  
23 816 are organized such that certain bits correspond to certain servers, sites, or  
24 services within the walled garden 420.  
25

1 In operation, the WGPS 414 examines the affiliation 815 and the set of bits  
2 representing the access rights of the user 816 to determine whether the user has  
3 rights to the specified walled garden 420 service. To make the latter  
4 determination, the WGPS 414 extracts the plot number from the HTTP request  
5 and uses it as an index into the set of bits 816 in the ticket 800. Brown instructs  
6 that the value of the indexed bit specifies whether the user is authorized to access  
7 the walled garden 420 service or site having the given plot number. This  
8 minimizes the overhead utilized to determine whether the ticket allows access.  
9 The WGPS 414 then either grants or denies 630 access to the user.

### 11 The Claims

12 **Claim 1** has been amended and recites a method of updating keys that  
13 decrypt login tickets that log a user into multiple sites, the method comprising [added  
14 language appears in bold italics]:

- 15 • generating a first key having a first version number;
- 16 • providing tickets encoded consistent with the first key, the ticket  
17 having a version number corresponding to the first version number;
- 18 • generating a second key having a second version number; and when  
19 the second key becomes current at a site, providing tickets encoded  
20 consistent with the second key, the ticket having a version number  
21 corresponding to the second version number;
- 22 • *wherein said tickets are configured to enable a user to access and  
23 use one or more affiliated servers without requiring any additional  
24 authentication information other than authentication information  
25 originally provided by the user to an authentication server.*

23 In making out the rejection of this claim, the Office argues that it is  
24 anticipated by Brown. Applicant respectfully disagrees, particularly in view of the  
25

1 amendment made above. Specifically, this claim now recites that the tickets are  
2 "configured to enable a user to access and use one or more affiliated servers without  
3 requiring any additional authentication information other than authentication  
4 information originally provided by the user to an authentication server." Support for  
5 this limitation can be found throughout Applicant's specification, particularly from  
6 page 7, line 4 through page 8, line 19 (e.g. "After registering and logging into the  
7 authentication server, the user can visit any affiliate server (i.e., affiliate servers that  
8 are also registered with the same authentication server) without requiring any  
9 additional authentication and without re-entering user information that is already  
10 contained in the associated user profile.").

11 Brown, on the other hand, discloses and teaches a method in which its tickets  
12 require authentication information in addition to authentication information  
13 originally provided by a user. For example, Brown's ticket comprises, as shown in  
14 Fig. 8, an affiliation portion 815 that contains a set of bits that represents the access  
15 rights of the user relative to individual certain servers, sites or services within  
16 Brown's walled garden. See, e.g. column 12, lines 13-22. The operation of Brown's  
17 method is described in more detail starting in column 6, line 34:

18  
19 Initially, the user uses the UI on the client 112 to request 610 access  
20 to a service in the walled garden 420. For example, the client 112 may  
21 generate a UI on the TV 110. The user, using the UI and an input device  
22 such as an IR keyboard, requests access to the service through the web  
23 browsing software 324 executing on the client 112. Alternatively, the client  
24 112 may be coupled to or integrated into a computer system and the user  
25 may use web browsing software to request access to a web site in the  
walled garden 420. As mentioned above, the request 610 from the client  
112 to the WGPS 414 preferably takes the form of a URL such as  
"http://wg/<plot number>/ . . . " In one embodiment, the user visits a web  
page or portal that references, either directly or indirectly, all of the

1 available walled garden services. When the user selects a link to a particular  
2 service, the web page directs the client 112 to the proper URL.

3 The WGPS 414 receives the request 610 and determines from the  
4 URL that the client is attempting to access a restricted service in the walled  
5 garden 420. Assume, however, that this request 610 is the first request from  
6 the client 112 to the WGPS 414. As a result, the client 112 did not include a  
7 ticket with the request 610. Therefore, the WGPS 414 denies 611 access to  
8 the walled garden 420 and sends a HTTP 407 response to challenge 612 the  
9 client 112 to supply the ticket in a subsequent request.

10 The client 112 receives the challenge 612. Preferably, the web  
11 browser then passes control to an authorization dynamic link library (DLL)  
12 executing on the client 112. *The authorization DLL creates the*  
13 *appropriate UI to let the user authenticate himself or herself to the client*  
14 *112.*

15 The authorization DLL then establishes a SSL connection with the  
16 GS 416 and makes a request 616 for the ticket by sending the user  
17 authentication information, as well as the Box ID of the client 112, across  
18 the SSL connection. *The GS 416 authenticates the user by validating 618*  
19 *the authentication information against the information in the database*  
20 *440.*

21 If the validation 618 is successful, the GS 416 preferably constructs  
22 620 the ticket. As shown in FIG. 8, the ticket 800 preferably includes the  
23 Box ID 810 of the client 112 requesting the ticket, a version number 812,  
24 an expiration date 814 (or duration when the ticket is valid), an affiliation  
25 815, and a set of bits representing the access rights of the user 816. The  
version number 812 is preferably a control number used by the GS 416 to  
ensure that the WGPS 414 properly interprets the ticket 800. The expiration  
date 814 can be any time in the future or a time span when the ticket 800 is  
valid and may range, for example, from a few minutes to a few hours. *The*  
*affiliation indicates the particular walled garden 420 or MSO to which*  
*the ticket 800 pertains. The set of bits representing the access rights of the*  
*user 816 are preferably organized such that certain bits correspond to*  
*certain servers, sites, or services within the walled garden 420.* In one  
embodiment of the present invention, the bits representing the access rights  
816 are run length encoded (RLE) to reduce the storage size of the field.  
Other information, such as the IP address of the client 112 and a timestamp  
may also be stored in the ticket 800.

1 Thus, Brown describes a method in which the user is first authenticated,  
2 and then a ticket is built that includes the affiliation portion 815. The affiliation  
3 portion is further used to authenticate that the user is authorized to use certain  
4 services within the walled garden. Thus, not only does Brown not anticipate the  
5 subject matter of this claim, Brown teaches directly away therefrom. Accordingly,  
6 for at least this reason, this claim is allowable.

7 **Claims 2-4** depend from claim 1 and are allowable as depending from an  
8 allowable base claim. These claims are also allowable for their own recited  
9 features which, in combination with those recited in claim 1, are neither disclosed  
10 nor suggested in the references of record, either singly or in combination with one  
11 another. In addition, given the allowability of claim 1, the further rejection of  
12 claim 2 over the combination with Curry is not seen to add anything of  
13 significance.

14 **Claim 5** has been amended and recites a computer readable medium having  
15 instructions stored thereon for causing a computer to perform a method of updating  
16 keys that decrypt login tickets that log a user into multiple sites, the method  
17 comprising [added language appears in bold italics]:

- 18
- 19 • generating a first key having a first version number;
- 20 • providing tickets encoded consistent with the first key, the ticket  
having a version number corresponding to the first version number;
- 21 • generating a second key having a second version number; and
- 22 • when the second key becomes current at a site, providing tickets  
encoded consistent with the second key, the ticket having a version  
23 number corresponding to the second version number;
- 24 • ***wherein said tickets are configured to enable a user to access and  
use one or more affiliated servers without requiring any additional  
25 authentication information other than authentication information  
originally provided by the user to an authentication server.***

1  
2 As noted above, Brown neither discloses nor suggests any such subject  
3 matter. More particularly, Brown teaches directly away from the subject matter of  
4 this claim. Accordingly, this claim is allowable.

5 **Claim 6** recites a method of generating keys that decrypt login tickets that  
6 log a user into multiple sites, the method comprising:

- 7
- 8 • generating a first key in the form of an executable having a first  
version number;
  - 9 • generating a second key in the form of an executable having a second  
version number; and
  - 10 • providing an indication to a login server identifying which key is  
current for each site such that the tickets are properly encoded.
- 11

12  
13 In making out the rejection of this claim, the Office argues that Brown  
14 discloses all features of the claim except for a key comprising key data and  
15 executable code for decrypting tickets. The Office then relies on See and cites to  
16 column 5, lines 29-36 in support therefore. Applicant respectfully disagrees and  
traverses the Office's rejection.

17 Preliminarily, Applicant notes that the claim recites that the subject keys  
18 are "*in the form of an executable*". The section of See relied on by the Office  
19 describes an authentication agent comprising a software module. The agent is  
20 described to comprise an address of a device 10, an address of basic server 320,  
21 and an authentication key for server 320. While the authentication agent may  
22 comprise executable code, it does not appear that See's authentication key is *in the*  
23 *form of an executable* as that term is contemplated in Applicant's disclosure.  
24  
25



1 As an example, consider Applicant's specification starting on page 9, line  
2 20. There, the specification states as follows:

3  
4 A key generator 345 is also associated with the authentication server.  
5 It has an administrative interface 350 that allows selection of new keys by a  
6 user, and provides keys in the form of an executable piece of code referred  
7 to as key.exe via a network 360 (shown in two places for convenience) such  
8 as the Internet, to one or more affiliate servers such as a partner site 370.

9 Accordingly, as this subject matter is neither disclosed nor suggested in the  
10 references cited by the Office, the Office has failed to establish a *prima facie* case  
11 of obviousness and this claim is allowable.

12 **Claims 7 and 8** depend from claim 6 and are allowable as depending from  
13 an allowable base claim. These claims are also allowable for their own recited  
14 features which, in combination with those recited in claim 6, are neither disclosed  
15 nor suggested in the references of record, either singly or in combination with one  
16 another.

17 **Claim 9** recites a computer readable medium having instructions stored  
18 thereon for causing a computer to perform a method of generating keys that decrypt  
19 login tickets that log a user into multiple sites, the method comprising:

- 20 • generating *a first key in the form of an executable* having a first  
21 version number;
- 22 • generating *a second key in the form of an executable* having a second  
23 version number; and
- 24 • providing an indication to a login server identifying which key is  
25 current for each site such that the tickets are properly encoded.

1  
2 The Office rejects this claim and uses the same arguments as were used in  
3 making out the rejection of claim 6. Applicant respectfully notes that neither  
4 Brown nor See disclose or suggest keys in the form of executables as  
5 contemplated in this claim. Accordingly, for at least this reason, the Office has  
6 failed to establish a *prima facie* case of obviousness and this claim is allowable.

7 **Claim 10** recites a system that generates keys that decrypt login tickets that  
8 log a user into multiple sites, the system comprising:

- 9
- 10 • a key generator that generates *a first key in the form of an executable*  
11 having a first version number and generates a second key in the form  
12 of an executable having a second version number; and
  - 13 • means for providing information to a login server identifying which  
14 key is current for each site such that the tickets are properly encoded.

15 The Office rejects this claim and uses the same arguments as were used in  
16 making out the rejection of claim 6. Applicant respectfully notes that neither  
17 Brown nor See disclose or suggest keys in the form of executables as  
18 contemplated in this claim. Accordingly, for at least this reason, the Office has  
19 failed to establish a *prima facie* case of obviousness and this claim is allowable.

20 **Claim 11** has been amended and recites a method of updating keys that  
21 decrypt login tickets that log a user into multiple sites, the method comprising [added  
22 language appears in bold italics]:

- 23
- 24 • generating a new key with an incremented version number;
  - 25 • sending the new key to a partner site for use in decoding tickets with  
the incremented version number;
  - updating key and version information for a login server; and

- generating tickets decodable by the new key when an indication that a key having a previous version number has expired;
- *wherein said tickets are configured to enable a user to access and use one or more affiliated servers without requiring any additional authentication information other than authentication information originally provided by the user to an authentication server.*

In making out the rejection of this claim, the Office argues that its subject matter is anticipated by Brown. Applicant disagrees, particularly in view of the amendment that has been made. As noted above, Brown neither discloses nor suggests this subject matter. In point of fact, Brown teaches directly away from such subject matter. As such, this claim is allowable.

**Claim 12** has been amended and recites a computer readable medium having instructions stored thereon for causing a computer to perform a method of updating keys that decrypt login tickets that log a user into multiple sites, the method comprising [added language appears in bold italics]:

- generating a new key with an incremented version number;
- sending the new key to a partner site for use in decoding tickets with the incremented version number;
- updating key and version information for a login server; and
- generating tickets decodable by the new key when an indication that a key having a previous version number has expired;
- *wherein said tickets are configured to enable a user to access and use one or more affiliated servers without requiring any additional authentication information other than authentication information originally provided by the user to an authentication server.*

In making out the rejection of this claim, the Office argues that its subject matter is anticipated by Brown. Applicant disagrees, particularly in view of the amendment that has been made. As noted above, Brown neither discloses nor

1 suggests this subject matter. In point of fact, Brown teaches directly away from  
2 such subject matter. As such, this claim is allowable.

3 **Claim 13** has been amended and recites a method of updating a key used to  
4 decrypt tickets used to log into a site, the method comprising [added language  
5 appears in bold italics]:

- 6
- 7 • receiving an updated key with a new version number;
- 8 • setting a time for an old current key having an old version number to  
9 expire;
- 10 • making the updated key the current key;
- 11 • *wherein said tickets are configured to enable a user to access and  
12 use one or more affiliated servers without requiring any additional  
13 authentication information other than authentication information  
14 originally provided by the user to an authentication server.*

15 In making out the rejection of this claim, the Office argues that the claim is  
16 rendered obvious over Brown in view of Olkin. Applicant respectfully disagrees  
17 particularly in view of the amendment in the present claim. Specifically, Brown  
18 neither discloses nor suggests and, in point of fact, teaches away from the subject  
19 matter of this claim. As such, the Office has failed to establish a *prima facie* case  
20 of obviousness and the combination with Olkin is not seen to add anything of  
21 significance. Accordingly, this claim is allowable.

22 **Claims 14 and 15** depend from claim 13 and are allowable as depending  
23 from an allowable base claim. These claims are also allowable for their own  
24 recited features which, in combination with those recited in claim 13, are neither  
25 disclosed nor suggested in the references of record, either singly or in combination  
with one another. In addition, given the allowability of claim 13, the further

1 rejection of claim 14 over the combination with See is not seen to add anything of  
2 significance.

3 **Claim 16** has been amended and recites a computer readable medium  
4 having instructions stored thereon for causing a computer to perform a method of  
5 updating a key used to decrypt tickets used to log into a site, the method comprising  
6 [added language appears in bold italics]:

- 7
- 8 • receiving an updated key with a new version number;
- 9 • setting a time for an old current key having an old version number to expire;
- 10 • making the updated key the current key;
- 11 • ***wherein said tickets are configured to enable a user to access and***  
12 ***use one or more affiliated servers without requiring any additional***  
***authentication information other than authentication information***  
***originally provided by the user to an authentication server.***

13 In making out the rejection of this claim, the Office argues that Brown  
14 discloses all of the features of the claim except for setting a time for an old current  
15 key having an old version to expire. The Office then relies on Olkin to supply this  
16 missing feature and argues that the claim is obvious in view of these references.

17 Applicant has amended this claim to recite that the tickets are configured to  
18 enable a user to access and use one or more affiliated servers without requiring any  
19 additional authentication information other than authentication information originally  
20 provided by the user to an authentication server. As noted above, Brown neither  
21 discloses nor suggests any such subject matter and, in point of fact, teaches directly  
22 away therefrom. As such, the Office's combination does not establish a *prima facie*  
23 case of obviousness and this claim is allowable.  
24  
25

1       **Claim 19** recites a method of managing keys used to decrypt tickets for  
2 logging onto a site, the method comprising:

- 3           • receiving a first key with a first version number;
- 4           • encrypting the first key using a hardware address;
- 5           • changing a current key variable to the first version number;
- 6           • receiving a new key with an incremented version number;
- 7           • encrypting the new key using a hardware address; and
- 8           • identifying the new key as the current key.

9       In making out the rejection of this claim, the Office argues that Brown  
10 discloses all of the features of the claim except for encrypting the first key and the  
11 new key using a hardware address. The Office then relies on Biran for this feature  
12 and argues that the combination of these references renders the subject matter of this  
13 claim obvious. Applicant respectfully disagrees and traverses the Office's rejection.

14       Biran discloses a system and method for address protection using a hardware-  
15 defined application key. In Biran, a protection block 48 holds a key 43 having a  
16 value that is a function of a physical address 41 of register 40 (see Fig. 3). Biran  
17 instructs that the key is hardware dependent and unique since the register with which  
18 the key is associated has a unique hardware address. Biran does not disclose or  
19 suggest ***encrypting any keys using a hardware address*** as recited in this claim. In  
20 fact, a thorough review of Biran indicates that the word "encrypt" does not occur in a  
21 single instance in its disclosure. The reason for this is self-evident—because Biran  
22 has nothing whatsoever to do with encrypting a key using a hardware address.

23       Accordingly, for at least this reason, the Office has failed to establish a *prima*  
24 *facie* case of obviousness and this claim is allowable.

1       **Claims 20-28** depend from claim 19 and are allowable as depending from  
2 an allowable base claim. These claims are also allowable for their own recited  
3 features which, in combination with those recited in claim 19, are neither disclosed  
4 nor suggested in the references of record, either singly or in combination with one  
5 another. In addition, given the Office's failure to establish a *prima facie* case of  
6 obviousness with respect to claim 19, the further rejections of claims 20-22 over  
7 Olkin, of claim 23 over Olkin and Wasserman, and claim 28 over Audebert are not  
8 seen to add anything of significance.

9       **Claim 26** recites a computer readable medium having instructions stored  
10 thereon for causing a computer to perform a method of managing keys used to  
11 decrypt tickets for logging onto a site, the method comprising:

- 12           • receiving a first key with a first version number;
- 13           • ***encrypting the first key using a hardware address;***
- 14           • changing a current key variable to the first version number;
- 15           • receiving a new key with an incremented version number;
- 16           • ***encrypting the new key using a hardware address;*** and
- 17           • identifying the new key as the current key.

18       In making out the rejection of this claim, the Office argues that Brown  
19 discloses all of the features of the claim except for encrypting the first key and the  
20 new key using a hardware address. The Office then relies on Biran for this feature  
21 and argues that the combination of these references renders the subject matter of this  
22 claim obvious. Applicant respectfully disagrees and traverses the Office's rejection.

23       Biran discloses a system and method for address protection using a hardware-  
24 defined application key. In Biran, a protection block 48 holds a key 43 having a  
25 value that is a function of a physical address 41 of register 40 (see Fig. 3). Biran

1 instructs that the key is hardware dependent and unique since the register with which  
2 the key is associated has a unique hardware address. Biran does not disclose or  
3 suggest *encrypting any keys using a hardware address* as recited in this claim. In  
4 fact, a thorough review of Biran indicates that the word “encrypt” does not occur in a  
5 single instance in its disclosure. The reason for this is self-evident—because Biran  
6 has nothing whatsoever to do with encrypting a key using a hardware address.

7 Accordingly, for at least this reason, the Office has failed to establish a *prima*  
8 *facie* case of obviousness and this claim is allowable.

9 **Claim 27** recites a method of updating keys used to decrypt tickets used to  
10 log into multiple sites on a network, the method comprising:

- 11 • generating a new key with a new version number to take the place of
- 12 an old key with an old version number;
- 13 • storing the new key on a site to be logged into by a user;
- 14 • changing a current key indication to the new key;
- 15 • allowing current logged in users to continue using the old key; and
- 16 • redirecting new users to a login server to obtain a ticket consistent with
- 17 the new key.

18 In making out the rejection of this claim, the Office argues that Brown and  
19 Audebert teach all of the features of this claim except for allowing current logged in  
20 users to continue using the old key. The Office then relies on Olkin for this subject  
21 matter and argues that its combination with Brown and Audebert renders the subject  
22 matter of this claim obvious. Applicant respectfully disagrees and traverses the  
23 Office’s rejection.

24 Applicant respectfully submits that the Office has mischaracterized Olkin.  
25 Specifically, the Office characterizes Olkin as disclosing a system that allows current



1 logged in users to use an old key and cites to column 9, lines 25-31 in support  
2 therefore. A careful reading of Olkin should indicate that the excerpt cited by the  
3 Office describes an expiration setting that allows an email sender to specify when the  
4 security server should discard a message key and thus make an associated email  
5 unreadable. The default to allowing the sender to provide an expiration setting is to  
6 discard the message key at some time in the future. Thus, after either situation (i.e.  
7 the user specifies the expiration or the system specifies the expiration), it would  
8 appear that any associated email would be unreadable. Thus, this excerpt does not,  
9 as the Office contends, disclose or suggest allowing current logged in users to  
10 continue using an old key. In each of Olkin's cases, it would appear that after a  
11 message key has expired, it is not functionally useable.

12 Accordingly, for at least this reason, the Office has failed to establish a *prima*  
13 *facie* case of obviousness and this claim is allowable.

14 **Claims 28-35** depend from claim 27 and are allowable as depending from  
15 an allowable base claim. These claims are also allowable for their own recited  
16 features which, in combination with those recited in claim 27, are neither disclosed  
17 nor suggested in the references of record, either singly or in combination with one  
18 another. In addition, in view of the Office's failure to establish a *prima facie* case  
19 of obviousness with respect to claim 27, the rejections of claim 29 over the  
20 combination with Wasserman, of claim 32 over Biran, and of claim 34 over See is  
21 not seen to add anything of significance.

22 **Claim 36** recites a computer readable medium having instructions stored  
23 thereon for causing a computer to perform a method of updating keys used to decrypt  
24 tickets used to log into multiple sites on a network, the method comprising:  
25

- generating a new key with a new version number to take the place of an old key with an old version number;
- storing the new key on a site to be logged into by a user;
- changing a current key indication to the new key;
- ***allowing current logged in users to continue using the old key***; and
- redirecting new users to a login server to obtain a ticket consistent with the new key.

The Office rejects this claim and makes arguments that are the same as those made with respect to claim 27. For all of the reasons set forth with respect to the Office's failure to establish a *prima facie* case of obviousness in the rejection of claim 27, this claim is allowable.

**Claim 37** has been amended and recites a method of logging on to multiple sites, the method comprising [added language appears in bold italics]:

- sending a first login ticket to a desired site, wherein the login ticket is encrypted to be decoded by a first key having a first version number;
- receiving an indication that the first key has expired;
- obtaining a second login ticket from an authentication server, wherein the second login ticket is encrypted consistently with a new key having a second version number; and
- sending the second login ticket to the site to log into the site;
- ***wherein said tickets are configured to enable a user to access and use one or more affiliated servers without requiring any additional authentication information other than authentication information originally provided by the user to an authentication server.***

In making out the rejection of this claim, the Office argues that it is anticipated by Brown. Applicant respectfully disagrees, particularly in view of the amendment made above. Specifically, this claim now recites that the tickets are "configured to enable a user to access and use one or more affiliated servers without

1 requiring any additional authentication information other than authentication  
2 information originally provided by the user to an authentication server.” Support for  
3 this limitation can be found throughout Applicant’s specification, particularly from  
4 page 7, line 4 through page 8, line 19 (e.g. “After registering and logging into the  
5 authentication server, the user can visit any affiliate server (i.e., affiliate servers that  
6 are also registered with the same authentication server) without requiring any  
7 additional authentication and without re-entering user information that is already  
8 contained in the associated user profile.”).

9 Brown, on the other hand, discloses and teaches a method in which its tickets  
10 require authentication information in addition to authentication information  
11 originally provided by a user. For example, Brown’s ticket comprises, as shown in  
12 Fig. 8, an affiliation portion 815 that contains a set of bits that represents the access  
13 rights of the user relative to individual certain servers, sites or services within  
14 Brown’s walled garden. See, e.g. column 12, lines 13-22. The operation of Brown’s  
15 method is described in more detail starting in column 6, line 34:

16  
17 Initially, the user uses the UI on the client 112 to request 610 access  
18 to a service in the walled garden 420. For example, the client 112 may  
19 generate a UI on the TV 110. The user, using the UI and an input device  
20 such as an IR keyboard, requests access to the service through the web  
21 browsing software 324 executing on the client 112. Alternatively, the client  
22 112 may be coupled to or integrated into a computer system and the user  
23 may use web browsing software to request access to a web site in the  
24 walled garden 420. As mentioned above, the request 610 from the client  
25 112 to the WGPS 414 preferably takes the form of a URL such as  
"http://wg/<plot number>/ . . . " In one embodiment, the user visits a web  
page or portal that references, either directly or indirectly, all of the  
available walled garden services. When the user selects a link to a particular  
service, the web page directs the client 112 to the proper URL.

The WGPS 414 receives the request 610 and determines from the  
URL that the client is attempting to access a restricted service in the walled

1 garden 420. Assume, however, that this request 610 is the first request from  
2 the client 112 to the WGPS 414. As a result, the client 112 did not include a  
3 ticket with the request 610. Therefore, the WGPS 414 denies 611 access to  
4 the walled garden 420 and sends a HTTP 407 response to challenge 612 the  
5 client 112 to supply the ticket in a subsequent request.

6 The client 112 receives the challenge 612. Preferably, the web  
7 browser then passes control to an authorization dynamic link library (DLL)  
8 executing on the client 112. *The authorization DLL creates the*  
9 *appropriate UI to let the user authenticate himself or herself to the client*  
10 *112.*

11 The authorization DLL then establishes a SSL connection with the  
12 GS 416 and makes a request 616 for the ticket by sending the user  
13 authentication information, as well as the Box ID of the client 112, across  
14 the SSL connection. *The GS 416 authenticates the user by validating 618*  
15 *the authentication information against the information in the database*  
16 *440.*

17 If the validation 618 is successful, the GS 416 preferably constructs  
18 620 the ticket. As shown in FIG. 8, the ticket 800 preferably includes the  
19 Box ID 810 of the client 112 requesting the ticket, a version number 812,  
20 an expiration date 814 (or duration when the ticket is valid), an affiliation  
21 815, and a set of bits representing the access rights of the user 816. The  
22 version number 812 is preferably a control number used by the GS 416 to  
23 ensure that the WGPS 414 properly interprets the ticket 800. The expiration  
24 date 814 can be any time in the future or a time span when the ticket 800 is  
25 valid and may range, for example, from a few minutes to a few hours. *The*  
*affiliation indicates the particular walled garden 420 or MSO to which*  
*the ticket 800 pertains. The set of bits representing the access rights of the*  
*user 816 are preferably organized such that certain bits correspond to*  
*certain servers, sites, or services within the walled garden 420.* In one  
embodiment of the present invention, the bits representing the access rights  
816 are run length encoded (RLE) to reduce the storage size of the field.  
Other information, such as the IP address of the client 112 and a timestamp  
may also be stored in the ticket 800.

26 Thus, Brown describes a method in which the user is first authenticated,  
27 and then its ticket is build that includes the affiliation portion 815. The affiliation  
28 portion is further used to authenticate that the user is authorized to user certain  
29

1 services within the walled garden. Thus, not only does Brown not anticipate the  
2 subject matter of this claim, Brown teaches directly away therefrom. Accordingly,  
3 for at least this reason, this claim is allowable.

4 **Claims 38-40** depend from claim 37 and are allowable as depending from  
5 an allowable base claim. These claims are also allowable for their own recited  
6 features which, in combination with those recited in claim 37, are neither disclosed  
7 nor suggested in the references of record, either singly or in combination with one  
8 another.

9 **Claim 41** has been amended and recites a computer readable medium  
10 having instructions stored thereon for causing a computer to perform a method of  
11 logging on to multiple sites, the method comprising [added language appears in bold  
12 italics]:

- 13 • sending a first login ticket to a desired site, wherein the login ticket is
- 14 encrypted to be decoded by a first key having a first version number;
- 15 • receiving an indication that the first key has expired;
- 16 • obtaining a second login ticket from an authentication server, wherein
- 17 the second login ticket is encrypted consistently with a new key having
- 18 a second version number; and
- 19 • sending the second login ticket to the site to log into the site;
- 20 • *wherein said tickets are configured to enable a user to access and*
- 21 *use one or more affiliated servers without requiring any additional*
- 22 *authentication information other than authentication information*
- 23 *originally provided by the user to an authentication server.*

24 In making out the rejection of this claim, the Office argues that it is  
25 anticipated by Brown. Applicant respectfully disagrees, particularly in view of the  
amendment made above. Specifically, this claim now recites that the tickets are  
“configured to enable a user to access and use one or more affiliated servers without

1 requiring any additional authentication information other than authentication  
2 information originally provided by the user to an authentication server.”

3 As noted above, not only does Brown not disclose or suggest this feature,  
4 Brown teaches directly away from this feature. Accordingly, this claim is allowable.

5 **Claim 42** has been amended and recites an encrypted ticket for use in  
6 logging on to a website, the ticket comprising [amended language appears in bold  
7 italics]:

- 8 • an unencrypted version number corresponding to a key version
- 9 number stored on the website; and
- 10 • an encrypted string identifying the website and information, which
- 11 when decrypted using the key having the same version number
- 12 authenticates the user for logging the user into the website;
- 13 • *wherein said ticket is configured to enable a user to access and use*
- 14 *one or more affiliated servers without requiring any additional*
- 15 *authentication information other than authentication information*
- 16 *originally provided by the user to an authentication server.*

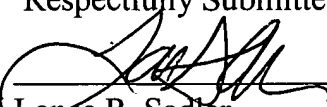
17 In making out the rejection of this claim, the Office argues that it is  
18 anticipated by Brown. Applicant respectfully disagrees, particularly in view of the  
19 amendment made above. Specifically, this claim now recites that the ticket is  
20 “configured to enable a user to access and use one or more affiliated servers without  
21 requiring any additional authentication information other than authentication  
22 information originally provided by the user to an authentication server.”

23 As noted above, not only does Brown not disclose or suggest this feature,  
24 Brown teaches directly away from this feature. Accordingly, this claim is allowable.  
25

1        **Conclusion**

2        Applicant respectfully submits that all of the claims are in condition for  
3 allowance. If the Office's next anticipated action is to be anything other than  
4 issuance of a Notice of Allowability, Applicant respectfully requests a telephone call  
5 for the purpose of scheduling an interview.

6  
7  
8        Dated: 4/9/04

Respectfully Submitted,  
By:   
Lance R. Sadler  
Reg. No. 38,605  
(509) 324-9256